

## CLAIMS

Having thus described our invention, what we claim as new and desire to secure by Letters Patent is as follows:

- Sub A2*
- 09617913.071700
- 1 1. A method for encrypting and decrypting data
  - 2 comprising steps of:
  - 3 generating a random number sequence;
  - 4 transmitting the random number sequence to a data
  - 5 encryption station and a data decryption station;
  - 6 generating a private key;
  - 7 inputting the private key to the data encryption
  - 8 station and to the data decryption station;
  - 9 selecting at the data encryption station an
  - 10 encryption subsequence from the random number sequence,
  - 11 the boundaries of the encryption subsequence based on the
  - 12 private key;
  - 13 encrypting a plaintext data at the data encryption
  - 14 station based on the private key and the selected
  - 15 encryption subsequence and generating, as a result, an
  - 16 encrypted data;
  - 17 transmitting the encrypted data from the encryption
  - 18 station to the decryption station;
  - 19 selecting at the data decryption station, based on
  - 20 the private key input to the decryption station, a
  - 21 decryption subsequence from the random number sequence,
  - 22 the boundaries of the decryption subsequence being
  - 23 identical to the boundaries of the encryption
  - 24 subsequence; and

25 decrypting the encrypted data at the data decryption  
26 station based on the private key and selection decryption  
27 sequence and generating, as a result, a recovered  
28 plaintext data.

22  
1 2. A method according to claim 1 further comprising  
2 steps of  
3 generating a synchronization signal;  
4 generating, at the encryption station, a first  
5 sampling time  $t$  based on the input private key;  
6 sampling the random number sequence at the  
7 encryption station for a predetermined interval beginning  
8 at a time based on  $t$ , to generate a sampled block of  
9 bits; and  
10 storing the sampled block of bits in a random number  
11 reservoir,  
12 wherein said encrypting step is based, in part, on a  
13 content of said random number reservoir.

1 3. A method according to claim 1, further comprising  
2 steps of:  
3 generating a synchronization signal;  
4 generating, at the encryption station, a sampling  
5 time  $t$  based on the input private key;  
6 sampling the random number sequence at the  
7 encryption station for a predetermined interval beginning  
8 at a time based on  $t$ , to generate a sampled block of  
9 bits;  
10 detecting a number of bits in said random number  
11 reservoir;

12 comparing the number of bits detected by said  
13 detecting step with a predetermined reservoir full value;  
14 and  
15 based on said comparing step detecting the number of  
16 bits in said random number reservoir being less than said  
17 predetermined reservoir full value, performing a step of  
18 storing the sampled block of bits in a random number  
19 reservoir,  
20 wherein said encrypting step is based, in part, on a  
21 content of said random number reservoir

1 4. A method according to claim 3 further comprising  
2 steps of:

3 based on said comparing step detecting the number of  
4 bits in said random number reservoir being less than said  
5 predetermined reservoir full value, performing steps of:

6 (a) generating a new private key based on the  
7 sampled block of bits and the previous private key;

8 (b) generating a new sampling time  $t$  based, at  
9 least in part, on the new private key;  
10 (c) sampling an additional block of bits from the  
11 random number sequence, at a sampling time based on the  
12 new sampling time  $t$ ;

13 (d) detecting a number of bits in said random  
14 number reservoir;

15 (e) comparing the number of bits detected by said  
16 detecting step with a predetermined reservoir full value;

17 (f) based on said comparing step detecting the  
18 number of bits in said random number reservoir being less  
19 than said predetermined reservoir full value, performing

a<sup>2</sup>

20 a step of storing the sampled additional block of bits in  
21 said random number reservoir; and  
22 (g) repeating steps (a) through (f) until said  
23 comparing step detects the number of bits in said random  
24 number reservoir as being greater than or equal to said  
25 predetermined reservoir full value.

002720 ETEZT960

1 5. A method according to claim 1 wherein said step of  
2 transmitting the random number sequence includes steps  
3 of:  
4 transmitting said random number sequence by uplink  
5 up to a satellite;  
6 transmitting said random number sequence received by  
7 said satellite down to said encryption station and to  
8 said decryption station.